Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

June 29, 2018

Cyber Supply Chain Risk Management: An Introduction

Introduction

A supply chain consists of the system of organizations, people, activities, information, and resources that provide products or services to consumers. Like other types of goods, a global supply chain exists for the development, manufacture, and distribution of information technology (IT) products (i.e., hardware and software). Recent media have highlighted the risks posed to IT from the supply chain.

In 2017, the U.S. Department of Homeland Security (DHS) ordered federal agencies to remove Kaspersky security products from their networks because of risk they posed. Legislation was subsequently enacted codifying that order. In addition, stories of persistent administrative passwords on devices or otherwise vulnerable products allowing unauthorized access to sensitive networks became more frequent.

This year, Congress is considering additional measures to promote cyber supply chain security (H.R. 5515 and S. 3085). Among other recent developments, DHS says they are investigating cyber supply chain security further; the Federal Communications Commission is considering prohibiting foreign telecommunications equipment for domestic use; and the U.S.-China Economic and Security Review Commission has issued a report highlighting supply chain concerns.

While interest in cyber supply chain security has increased recently, there have been other periods of intense scrutiny on supply chain issues. In 2012, for example, the White House issued a report on global supply chain security; the House Permanent Select Committee on Intelligence (HPSCI) released an unclassified report on threats from Chinese multinational companies Huawei and ZTE; ZTE was exposed selling phones in the United States with backdoor access; the Director of National Intelligence (DNI) cited supply chain security as a major threat in the Worldwide Threat Assessment; and the Government Accountability Office (GAO) studied the issue.

This InFocus reviews cyber supply chain risks, discusses ways in which they are currently managed, and provides issues that Congress may consider.

Cyber Supply Chain Risks

One way to view risks to cyber supply chain security is through the threat actors, their motivations, and ways in which they may compromise technology. DNI identified Russia, China, Iran, and North Korea as cyber threat nations. However, in their report on Department of State telecommunications, GAO highlights that technology is manufactured worldwide and vulnerabilities may be inserted by other actors. Some of those actors may include foreign intelligence services, malicious insiders, or criminals. These actors may be motivated to steal intellectual property, tamper with products, insert counterfeit goods, gain unauthorized access, sell extraneous access, or manipulate the operation of technology. They may accomplish their goals through inserting malicious code in software, manipulating hardware, or a combination of the two.

Cyber supply chain risks do not solely result from malicious human interference. The National Institute of Standards and Technology (NIST) finds that natural disasters may impede delivery of critical network components; poor quality assurance and engineering practices from vendors may provide deficient products; or an entity's own business practices may result in seeking, buying, and managing sub-par goods. These threats may result in data loss, modification, or exfiltration; system failures; or unavailable products.

Managing Risks

NIST defines cyber supply chain risk management (C-SCRM) as "the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of [IT] product and service supply chains." This definition distinguishes C-SCRM as an ongoing activity, rather than a single task, and accounts for the procurement and maintenance of hardware and software.

NIST Special Publication 800-161 provides guidance to federal agencies for how they may go about implementing risk management practices. They recommend that C-SCRM should align with an organization's existing risk management framework. Activities for risk management include cataloguing current systems and business practices, surveying systems for vulnerabilities, and developing processes to mitigate those vulnerabilities on an ongoing basis.

Just because a risk could possibly manifest, does not mean that it always exists, nor is it managed as if it perpetually exists. Instead, managers accept that risk is not binary but exists on a spectrum. This perspective pushes managers to consider how they are most at risk and prioritize mitigation strategies. This defense-in-depth strategy accepts that complete security is not guaranteed, but can lead system administrators to deploy tools effectively so that they can detect unwanted activity and stop damages from compounding.

Attackers may not know which defensive strategies are deployed on the systems where their compromised IT is installed. This uncertainty creates the possibility that purposefully embedding vulnerabilities in technology will

be detected and exposed, perhaps incriminating the attacker and stopping their plans. The chance of exposure is a consideration attackers evaluate when seeking to mass-compromise technology—and may incentivize them to pursue specific attacks against deliberate targets instead.

Conceptualizing risk is challenging because entities may not have threat information available to them, may lack an appreciation of their own vulnerabilities, or lack a framework to take that information and make resource decisions with it. For entities with general risk management programs, they may not have relevant expertise in IT products and threats to apply their established risk management practices to the supply chain. The prioritization of risk management requires that entities understand their own weaknesses, why they may be targeted, who or what may target them, and how. In order to extend these principles to their supply chain, entities will also need information on their vendors and suppliers, threat tactics, and best practices to mitigate risk.

Potential Issues For Congress

Generally, risk profiles (e.g., risk tolerance, resource allocations, vulnerabilities, threats, etc.) and risk management are unique from one entity or sector to another. This makes managing risk an activity which is individualized for each entity or sector. However, there are policy areas in which Congress may act with regard to C-SCRM that can affect federal activities.

Clarity of Responsibility

Federal IT management is dispersed among many federal agencies. The Office of Management and Budget (OMB) creates strategic guidance, NIST create documents describing implementation, DHS helps agencies with security management, and agencies themselves have to implement information security programs. Congress may consider creating specific responsibilities for federal or national supply chain security and assign those responsibilities across agencies or to a single federal entity. Rather than assign a single federal agency with all responsibilities for supply chain security, Congress may identify unique responsibilities and parse those out to agencies; such as intelligence gathering, technical expertise, the development and promulgation of defensive measures, and coordinating federal efforts. While this approach may provide clarity, its effectiveness may depend on the scope of authority Congress grants and resource allocations to the designated entity or entities.

Increased Awareness

The federal government may increase the information available from open and restricted government sources to all agencies and the information technology sector. To assist with increased awareness, the federal government could undertake activities to better understand the business relationships involved in the design or delivery of an IT product or service, and assess those businesses for potential risks. Rather than barring corporate activity, the government could then alert industry and consumers of those risks so that they may make informed decisions on whether and how they may use those products or services. This may help agencies better assess their own risk, and allow the companies to directly mitigate vulnerabilities in their products. Such a strategy recognizes that government is positioned to support the private sector, which has different responsibilities and greater control over technology.

Oversight

As part of annual oversight, Congress may ask agencies about their C-SCRM programs, their effectiveness, and challenges. Congress may also require such programs. In performing agency oversight, Congress may request a review and report by an agency into how it assesses and manages cyber supply chain risks. This review could inform future congressional activity and impel agencies to consider these issues and document their plans.

An example of such oversight is the Wolf Provision (found in Section 514 of Division B of P.L. 115-141 the Commerce, Justice, Science, and Related Agencies Appropriations Act, 2018). The National Aeronautics and Space Administration (NASA) Inspector General has an audit of NASA's implementation of the provision.

Prohibition on Specific Companies

As with the Kaspersky products, Congress may ban a certain company's products from being purchased or used at federal agencies. While such a prohibition may limit exposure to specific perceived risks posed by a product, set of products, or a company's work, complexities of the global cyber supply chain, business relationships, corporate restructuring, and other factors may inhibit the intended effectiveness. Such prohibitions have also faced court challenges regarding the banned company's due process and laws against bills of attainder.

Single Evaluator

Currently, agencies are responsible for evaluating risks posed by IT for themselves. However, some agencies lack the capability or capacity to perform thorough evaluations of their systems for supply chain risks. An option for Congress would be to assign a single federal agency the responsibility to evaluate supply chain risks in IT for all other agencies. This agency would examine IT hardware and software for potential risks. In order to do so, the agency would likely need access to threat intelligence, technical expertise, business relationships of the vendors, building products, and security experts, among other factors.

This strategy would align with the Administration's initiative to increase shared services. FedRAMP is a program Congress may look to in establishing such a program. In FedRAMP, one agency evaluates cloud service providers and creates documentation on the security of those services available to all agencies. This avoids the duplicate efforts of every agency examining the same product, and allows agencies to assess the product relative to their specific concerns.

Chris Jaikaran, cjaikaran@crs.loc.gov, 7-0750

IF10920